# LETTER FROM THE AUDITOR OF PUBLIC ACCOUNTS
# FINANCE AND ADMINISTRATION CABINET

## In Reference to the Statewide Single Audit of the Commonwealth of Kentucky

## For the Year Ended June 30, 2002


**EDWARD B. HATCHETT, JR.**
**AUDITOR OF PUBLIC ACCOUNTS**
**www.kyauditor.net**

**144 CAPITOL ANNEX**
**FRANKFORT, KY 40601**
**TELEPHONE (502) 564-5841**
**FACSIMILE (502) 564-2912**

**CONTENTS**

**CONTENTS**

EDWARD B. HATCHETT, JR.
AUDITOR OF PUBLIC ACCOUNTS

To the People of Kentucky
Honorable Paul E. Patton, Governor
Gordon C. Duke, Secretary
Finance and Administration Cabinet

# MANAGEMENT LETTER

This letter presents the results of our audit of the Finance and Administration Cabinet, performed as part of our annual statewide single audit of the Commonwealth of Kentucky.

In planning and performing our audit of the financial statements of the Commonwealth for the year ended June 30, 2002, we considered the Finance and Administration Cabinet's internal control in order to determine our auditing procedures for the purpose of expressing an opinion on the financial statements and not to provide assurance on internal control. We noted certain matters involving internal control, compliance and its operation that we are including in this letter. Some are considered to be reportable conditions under standards established by the American Institute of Certified Public Accountants.

Reportable conditions involve matters coming to our attention relating to significant deficiencies in the design or operation of internal control that, in our judgment, could adversely affect the Finance and Administration Cabinet's ability to record, process, summarize, and report financial data consistent with the assertions of management in the financial statements.

A material weakness is a reportable condition in which the design or operation of one or more internal control components does not reduce to a relatively low level the risk that errors or irregularities in amounts that would be material in relation to the financial statements being audited may occur and not be detected within a timely period by employees in the normal course of performing their assigned functions.

Our consideration of the internal control would not necessarily disclose all matters in the internal control that might be reportable conditions and, accordingly, would not necessarily disclose all reportable conditions that are also considered to be material weaknesses as defined above. However, none of the reportable conditions described herein is believed to be a material weakness.

144 CAPITOL ANNEX
FRANKFORT, KY 40601-3448
502.564.5841
FACSIMILE 502.564.2912
ehatchett@kyauditor.net



105 SEA HERO ROAD, SUITE 2
FRANKFORT, KY 40601-5404
502.573.0050
FACSIMILE 502.573.0067

To the People of Kentucky
Honorable Paul E. Patton, Governor
Gordon C. Duke, Secretary
Finance and Administration Cabinet

Some findings are Other Matters that we have included in this letter to communicate with management in accordance with Government Auditing Standards.

Included in this letter are the following:

- Acronym List
- Findings (Reportable, Material, and Other Matters)
- Summary Schedule of Prior Year Audit Findings

We have issued an unqualified opinion in our Statewide Single Audit of Kentucky that contains the Finance and Administration Cabinet findings, as well as those of other agencies of the Commonwealth. This report can be viewed on our website at www.kyauditor.net.

This letter is intended solely for the information and use of management and federal awarding agencies and pass-through entities, is not intended to be, and should not be used by anyone other than these specified parties.

Respectfully submitted,

Edward B. Hatchett, Jr.
Auditor of Public Accounts

## LIST OF ABBREVIATIONS/ACRONYMS

| | |
|---|---|
| AFR | Annual Financial Report |
| AIL | Agency Implementation Lead |
| AMS | American Management Systems |
| APA | Auditor of Public Accounts |
| BRASS | Budget Reporting and Analysis Support System |
| CAFR | Comprehensive Annual Financial Report |
| CAMRA | Complete Asset Management Reporting and Accounting System |
| CFDA | Catalog of Federal Domestic Assistance |
| CFR | Code of Federal Regulations |
| CIM | Compaq Insight Management Web Agents |
| CMIA | Cash Management Improvement Act |
| Commonwealth | Commonwealth of Kentucky |
| DBA | Database Administrators |
| DoS | Denial of Service |
| DMPS | Division of Material and Procurement Services |
| DSAS | Division of Statewide Accounting Services |
| FAC | Finance and Administration Cabinet |
| FAS | Financial Analysis System |
| FAS.V2 | Financial Analysis System Version Two |
| FDAC | Federal Domestic Assistance Catalog Division |
| FRT | Finacial Reporting Team |
| FTP | File Transfer Protocol |
| FY | Fiscal Year |
| GAAP | Generally Accepted Accounting Principles |
| GASB | Governmental Accounting Standards Board |
| GOPM | Governors Office for Policy and Management |
| GOT | Governor's Office for Technology |
| GWPN | Government Wide Project Number |
| HTTP | Hypertext Transfer Protocol |
| HTTPS | Hypertext Transfer Protocol Over Secure Socket Layer |
| JVB | Journal Voucher Correction |
| KAR | Kentucky Administrative Regulation |
| KRS | Kentucky Revised Statute |
| LAN | Local Area Network |
| LSA | Local Security Authority |
| MARS | Management Administrative Reporting System |
| MRDB | Management Reporting Database |
| N/A | Not Applicable |
| NT | New Technology |
| OFM | Office of Financial Management |
| OMB | Office of Management and Budget |
| OTS | Office of Technology Service |
| PD | Procurement Desktop |
| PDC | Primary Domain Controller |
| RACF | Resource Access Control Facility |
| RCW | Record of Control Weakness |
| RDS | Remote Document System |
| SAS | Statistical Analysis System |

## LIST OF ABBREVIATIONS/ACRONYMS

| | |
|---|---|
| SIP | State Investment Pool |
| SNMP | Simple Network Management Protocol |
| SQL | Structured Query Language |
| TSA | Treasury-State Agreement |
| WAN | Wide Area Network |

## FINANCIAL STATEMENT FINDINGS

***Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance***

### FINDING 02-FAC-1: The Finance And Administration Cabinet Should Closely Monitor The Progress Of The Disparity Study Relating To Set-Aside Laws

During our audit of the CAFR for FY 99, we reported that policies and procedures related to Small or Minority Business Set-Aside Laws were not being implemented by the Finance and Administration Cabinet (FAC), Division of Contracting and Administration. Our audit follow-up to this finding for FY 00 determined that no further action had been taken since our initial finding. In response to this FY 99 finding, FAC management responded that a Disparity Study (Study) was a necessary measure for implementing set-aside laws. FAC contracted with an outside vendor to conduct the Study. The Study was to be released February 2001 and no later than March 2001. In FY 01, during our follow-up to this finding, FAC responded that the Study had not been finalized, and it was anticipated that the Study would be completed in the near future. That was as of May 1, 2002.

Based on information obtained during FY 02 follow-up, as of November 1, 2002, the Study had yet to be completed. In addition, we have determined that FAC has paid approximately $590,000 to the firm contracted to complete the Study over the past three (3) fiscal years.

#### Recommendation

We recommend FAC determine the reasons the Study has not been completed. We further recommend FAC either take the necessary actions recommended by the Study, if feasible, or implement procedures to comply with the Small or Minority Business Set-Aside Laws.

#### Management's Response and Corrective Action Plan

*The Finance and Administration Cabinet is in the process of providing additional data to Griffin and Strong, the consultant for the Disparity Study, for inclusion in their report. Our timeline is to provide this data to Griffin and Strong by the end of December 2002. Griffin and Strong is committed to finalizing the Disparity Study and issuing the final report by the end of January 2003. When the Disparity Study is complete the Finance and Administration Cabinet will develop an action plan to implement findings, when feasible, to comply with KRS 45A.675.*

#### Auditor's Reply

Subsequent to FAC's response to this finding, the Study was released. We will review the report and the actions taken by FAC as a result of the study in the upcoming audit.

## FINANCIAL STATEMENT FINDINGS

***Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance***

### FINDING 02-FAC-2: The Finance And Administration Cabinet Should Ensure Consistent Classification And Categorization Of Investments In The Cash And Investment Note

The FAC CAFR team prepares the Cash and Investments note (Note 5). The CAFR team uses a confirmation database to compile summary sheets for each component unit of the Commonwealth. The confirmation database includes Management Administrative Reporting System (MARS) account numbers, funds, agency numbers, cash balances, cash on hand, book values for short and long term investments, and market values for short- and long-term investments. The summary sheets for each component unit provide cash and investments classifications and categorizations. In reviewing Note 5 information for each component unit, problems were noted in the classification and categorization of cash and investments. Those problems are summarized below.

*Classification*

In reviewing the summary sheets prepared by FAC, we noted some classification errors in FY 01. This year we noted the same problem. For example, although there has been significant improvement since last year, the State Investment Pool (SIP) funds were still not handled consistently between cash and investments classifications. FAC reported the SIP funds in two (2) different ways. Sometimes SIP cash and investments were reported as a total under investments. Other times, the SIP cash was reported as cash on the summary sheet, and the SIP investments were reported as a separate line item under investments. The SIP cash should be shown in the cash section of the summary sheet, and the investments should be shown in the investments section of the summary sheet.

Also, some funds were not classified as the correct type of investment. For example, commercial paper was classified as a non-negotiable certificate of deposit for the Kentucky Infrastructure Authority.

Improper classification could cause the Note 5 cash or investment balances to be overstated or understated. Although the total cash and investments reported on the Statement of Net Assets is correct, the individual cash and investment categories (current/noncurrent) would be misstated. In effect, this could mislead a user as to the liquidity and asset allocation of the Commonwealth's SIP.

Improper classification of cash and investment types would cause the Note 5 disclosure to not agree with the classification of cash and investments reported in the Statement of Net Assets. This could mislead a user as to the liquidity and asset allocation of the Commonwealth's cash and investment portfolio holdings.

## FINANCIAL STATEMENT FINDINGS

***Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance***

**FINDING 02-FAC-2: The Finance And Administration Cabinet Should Ensure Consistent Classification And Categorization Of Investments In The Cash And Investment Note (Continued)**

*Classification (Continued)*

According to the Implementation Guide for the Governmental Accounting Standards Board (GASB) 9, Footnote 5, Reporting Cash Flows of Proprietary and Nonexpendable Trust Funds and Governmental Entities That Use Proprietary Fund Accounting,

> . . . cash includes not only currency on hand, but also demand deposits with banks or financial institutions. Cash also includes deposits in other kinds of accounts or cash management pools that have the general characteristics of demand deposit accounts in that the governmental enterprise may deposit additional cash at any time and also withdraw cash at any time without prior notice or penalty . . ..

In relation to this issue, question 15 of the Implementation Guide states, " . . . the equity in an internal cash management or investment pool should not be considered cash unless the funds can be withdrawn at any time without prior notice or penalty . . .."

Moreover, question 15 notes for cash flow reporting purposes, the equity in a pool that is sufficiently liquid to enable withdrawal without prior notice or penalty should be treated as cash, and otherwise the equity should be considered an investment.

Good internal controls dictate that investments be classified correctly according to type.

*Categorization*

In reviewing the summary sheets prepared by FAC, some categorization errors were noted again this year, although improvement was made over the prior year. For example, SIP cash should be listed as category 1 cash/cash equivalents. However, on the Insurance Administration's summary sheet, this amount was listed as category 3 cash. Similarly, the University of Louisville's category 3 investments were listed as category 1 investments. Both of these items were corrected prior to the release of the CAFR.

Improper categorization could cause Note 5 cash and/or investments to be overstated/understated, which could mislead the user about the credit risk for a particular investment.

## FINANCIAL STATEMENT FINDINGS

***Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance***

**FINDING 02-FAC-2: The Finance And Administration Cabinet Should Ensure Consistent Classification And Categorization Of Investments In The Cash And Investment Note (Continued)**

*Categorization (Continued)*

According to GASB 3 Implementation Guide, *Deposits with Financial Institutions, Investments (including Repurchase Agreements), and Reverse Repurchase Agreements,* Question 4, provides there are three (3) credit risk categories used to report cash and investments information depending on "who the securities custodian is and how the securities custodian holds the security."

The categories required for reporting are as follows:

1. The custodian is the government's agent and is not the counterparty or the counterparty financial institution's trust department. The custodian holds the securities in the government's name.

2. The custodian is the counterparty financial institution's trust department or the counterparty's agent and the custodian holds the securities in the government's name.

3. The custodian is the counterparty, regardless of whether it holds the securities in government's name.

OR the custodian is the counterparty financial institution's trust department or the counterparty's agent and the custodian does not hold the securities in the government's name.

If the investment is not insured or registered or if collateral or investment is not in the possession of the government, then the investment is required to be categorized in one of the above categories.

**Recommendation**

*Classification*

Although we noted significant improvement in the proper classification of SIP cash, we recommend FAC set a specific policy on the classification of SIP cash and investments and inform component units and their auditors of the policy.

*Categorization*

We recommend consistent and proper categorization of investments for each component unit for Note 5, as required by GASB 3.

## FINANCIAL STATEMENT FINDINGS

***Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance***

**FINDING 02-FAC-2: The Finance And Administration Cabinet Should Ensure Consistent Classification And Categorization Of Investments In The Cash And Investment Note (Continued)**

### Management's Response and Corrective Action Plan

*We agree that the Finance and Administration Cabinet should be more consistent in categorization and classification of cash and investments. We believe most problems this year occurred primarily because of the implementation of GASB 35 by the universities. The revised AFR [Annual Financial Report] forms and confirmation report should provide more uniformity and consistency in the future. Our policy is to report state investment pool cash and investments exactly as the component units report them.*

## FINANCIAL STATEMENT FINDINGS

***Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance***

**FINDING 02-FAC-3: The Finance And Administration Cabinet Should Develop And Consistently Apply Formal Change Management Control Procedures For The Commonwealth's Cash And Investments Statistical Analysis System Programs**

As noted in the prior year's audit, the FAC, Office of Financial Management (OFM) did not develop formal program change management policies and procedures. During FY 02, the batch programs processed to generate cash and investment reports were rewritten in the Statistical Analysis System (SAS) language. These programs, implemented in May 2002, are critical to processing and reporting the Commonwealth's investments and to the Complete Asset Management, Reporting, and Accounting (CAMRA) system.

Prior to implementing the new SAS programs, OFM had designed and implemented a program change request form to reflect the necessity of modifications, description of modifications, testing of modifications, and authorization to implement modifications. However, our testing revealed seven (7) instances where modifications were made to program code without a supporting program modification request or other form of documented authorization. Further, complete formal policies and procedures for program change management were not developed.

Our examination of the program modification process also revealed several instances where acceptable business practices for system development were not employed for these SAS programs.

Prior to the development of the SAS programs, formal program specifications were not provided to the programmer by OFM management.

A separate library is not used for testing the SAS programs. All SAS test and production programs are housed in the same library. Further, the programmer has 'write' access to this library. The term library in this context means the same personal folder, on the same drive of one (1) server.

The SAS program code required recurring manual modifications. These modifications caused the programmer to regularly enter accounting data directly into programs without following OFM's established program modification procedures and without supervisory review.

The programmer has 'write' access to production data files, as well as the production programs.

Without formalized controls over program modifications, management increases the risk that incorrect or unauthorized changes could be moved into the live environment and adversely affect system processing results. Failure to follow best practices when developing new programs or systems can result in inaccurate or inefficient programs, or processing that does not adequately address security concerns for program modifications.

## FINANCIAL STATEMENT FINDINGS

***Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance***

**FINDING 02-FAC-3: The Finance And Administration Cabinet Should Develop And Consistently Apply Formal Change Management Control Procedures For The Commonwealth's Cash And Investments Statistical Analysis System Programs (Continued)**

### Recommendation

We recommend OFM develop and implement complete formalized program change management control policies and procedures to ensure consistent procedures are followed for authorization and approval of program changes, understanding of program objectives, control and maintenance of test and production libraries, transfer of changes to production, proper segregation of duties for programmers, and supervisory responsibilities over programmer access. Further, OFM should follow best practices when developing or revamping a program or system.

### Management's Response and Corrective Action Plan

*The Office of Financial Management has tried to incorporate the auditors input on the rewriting of our accounting software from the very beginning.*

*Formal program specifications were not given to the programmer. What was given to him was the task of replacing an existing system that had been audited by APA.*

*OFM is restructuring the read and write capabilities of all members. The programmer will not have write capabilities for production programs. Any program changes made in the future will be audited by our internal auditor to insure that only the requested and approved changes have been made.*

*Initially some manual entries were made into the program. As times goes forward automation is added to the program. At no time was the programmer able to enter data into the system without supervision and audits of output afterwards. Three staff members checked the data produced by the program. Our ultimate goal is to automate all entries.*

*At the recommendation of the auditors any program changes made must go through a four-stage process. Before the change is begun a supervisor must determine that a change is required. The supervisor then must check off how the programmer is going to make the change. After the change is made OFM's internal auditor audits the changes that have been made and writes a report on changes made. At this point it goes back to the supervisor for final authority to integrate the change into the production file.*

## FINANCIAL STATEMENT FINDINGS

***Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance***

**FINDING 02-FAC-3: The Finance And Administration Cabinet Should Develop And Consistently Apply Formal Change Management Control Procedures For The Commonwealth's Cash And Investments Statistical Analysis System Programs (Continued)**

**Management's Response and Corrective Action Plan (Continued)**

*OFM continues to strive to make the programming and maintenance of the programs correct and protected from unauthorized changes. We have already made some of the changes recommended by the APA and will shortly have all suggestions completed.*

## FINANCIAL STATEMENT FINDINGS

***Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance***

### FINDING 02-FAC-4: The Office Of Financial Management Should Improve Segregation Of Duty Controls

During the cash and investments audit for FY 02, OFM did not employ proper segregation of duties between programmer, operator, and librarian functions. In May 2002, SAS programs were implemented to replace a number of EXCEL and ACCESS applications that performed accounting and reporting functions for the Commonwealth's cash and investments. The programmer employed to develop and maintain the SAS programs was provided access to production programs and data. Further, he performed several tasks deemed to be incompatible with the standard tasks of a programmer. Our review specifically noted the following:

- The program code that performs monthly processing requires the programmer to manually enter critical accounting data directly into the program. The data consists of payoff balances and adjustment amounts for each investment pool and security lending balances for the month. Available supporting documentation was not deemed sufficient to substantiate these entries. Further, the documentation did not provide evidence of supervisory review.

- The programmer manually compiles the files that are input to the program that performs month-end processing.

- For the months of May and June, the programmer manually modified daily balances for float accounts within the data file that is input to the program that performs month-end processing. The fee amounts that are calculated on these balances were not recalculated based on the modified balances. Documentation provided as support for modified balances did not document evidence of authorization or supervisory review.

- From correspondence with OFM staff, it appears the programmer had manually modified the text files for the months of May and June that are input into MARS for creation of the monthly journal voucher document.

- Programs in development or testing are not controlled or segregated from the programs that are in production. Both test and production programs and data files are maintained on the programmer's personal network drive. Hence, the programmer has "write" access to the directory housing production programs and data. Further, the programmer acts as the operator for these programs. He submitted these programs for processing on a routine basis.

## FINANCIAL STATEMENT FINDINGS

***Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance***

### FINDING 02-FAC-4: The Office Of Financial Management Should Improve Segregation Of Duty Controls (Continued)

Employing strong segregation of duty controls decreases the opportunity for unauthorized modification to files and programs and the likelihood of losses occurring from incorrect use of data, programs, and other resources. Programmer duties should not include the input of accounting data. Program developers should be restricted from the production environment, and their activities should be conducted solely on "test" data. This will assist in ensuring an independent and objective testing environment without jeopardizing the integrity of production data. Computer operators should not have direct access to program source code. This will help ensure the computer operator does not intentionally or unintentionally introduce source code that has not been properly tested, and will lessen the opportunity of introducing malicious program code. Smaller organizations that cannot easily segregate programmer duties from development and operations should implement strict evaluation, authorization and approval procedures. Programmer activities in these circumstances should be closely monitored.

#### Recommendation

We recommend OFM take the necessary actions to discontinue the processes that allow programmer access to production programs and data. OFM should also eliminate procedures requiring the programmer to input accounting information into production programs. OFM should take the following actions to employ proper segregation of duty controls:

- Request modification to the program code that performs month-end processing to eliminate the need to manually enter accounting data. The programs should be developed to call in text or other input files generated by accounting personnel.

- Request a program be developed that will automate the compilation of daily files into the monthly text files that are input to the month-end SAS program.

- Separate the testing and production libraries and eliminate the programmer's update access to production programs and data.

- Control transfers from the testing environment to production and ensure another staff member is designated as librarian to perform this task following sufficient testing and authorized approval of the program.

## FINANCIAL STATEMENT FINDINGS

***Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance***

**FINDING 02-FAC-4: The Office Of Financial Management Should Improve Segregation Of Duty Controls (Continued)**

**Recommendation (Continued)**

Circumstances of an emergency nature requiring the programmer to have update access privileges should be documented and closely monitored at the appropriate supervisory level. For those circumstances when it is necessary to grant update access to a program or production data, a log should be created that specifically documents the individual accessing the production library by user ID (Identification), time of entry, specific programs, and data accessed and purpose. All activity should be subject to supervisory control, and system log entries should be substantiated by a formal request for the access granted.

**Management's Response and Corrective Action Plan**

*The program code was written with some flexibility to allow for unforeseen adjustments. Adjustments made using the manual process are calculated and entered by more than one person. The results are then checked by multiple individuals. The amounts entered into the month end adjustments had been calculated by the accounting staff. We do not see an issue with the programmer manually compiling files at the end of the month. We would need specifics as to what problems the auditors have and would then correct them.*

*Program development was changed in mid-July, 2002. A library was set up with access limited to an administrator who is not the programmer. Prior to mid-July programs were renamed when tested and were checked by our internal auditor. OFM has now set up a separation so the programmer is unable to access the production program.*

*All program changes are approved by his supervisor and changes audited by the Office of Financial Management's internal auditor. Only at this point in time is the new production program loaded into the library by the librarian. Programs are saved at the end of each month under a unique name for audit purposes. Automation of programs continues to be developed. All accounting data is generated by CAMRA and loaded into our SAS programs. This is an update since the end of the fiscal year.*

## FINANCIAL STATEMENT FINDINGS

***Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance***

**FINDING 02-FAC-5: The Finance And Administration Cabinet Should Work With American Management Systems To Strengthen Logical Security Measures Over The Management Administrative Reporting System And The Management Reporting Database**

FAC did not adequately control logical security access of the Management Reporting Database (MRDB) or the Procurement Desktop (PD) and Budget Reporting and Analysis Support System (BRASS) applications.

PD is a "two-tier" security system. The initial security level is the Commonwealth's Resource Access Control Facility (RACF). RACF determines which application systems and libraries an employee can access, and whether inquiry, alter, or update access will be allowed. Once the user accesses an application, their capabilities are controlled by the PD application. The PD application creates purchase requests; creates and issues solicitations from vendors, if necessary; awards and manages award documents, such as contracts, purchase orders, delivery orders, and master agreements; tracks the receipt of goods and services; and, creates and manages payable documents. The security features of password expiration, a lockout based on a number of unsuccessful attempts, and prevention of consecutive password usage have not been made available by the vendor American Management Systems (AMS), for this application. This application does allow for an expiration date to be entered for a PD user ID; however, this feature is not utilized for each user for it would not be feasible to have user's IDs expire on a regular basis.

BRASS is administered through the Governor's Office for Policy and Management and is the only component of MARS that uses a unique, three-character user ID that is separate and distinct from the RACF ID. The security features of password expiration, a lockout based on a number of unsuccessful attempts, and disallowance of consecutive password usage has not been made available by AMS for this application. After three (3) unsuccessful attempts, the application will close, but the user is not restricted from launching the application again and using the same ID with a different set of passwords.

MRDB is not an application of MARS, but a database that interacts with MARS applications to consolidate data so reports can be generated. These MARS applications include Advantage Financial, PD, and BRASS. A valid RACF ID is needed in order to access MRDB. However, a password security expiration feature has not been implemented for MRDB. The only restriction on password usage is reuse of passwords, which is not allowed.

## FINANCIAL STATEMENT FINDINGS

***Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance***

**FINDING 02-FAC-5: The Finance And Administration Cabinet Should Work With American Management Systems To Strengthen Logical Security Measures Over The Management Administrative Reporting System And The Management Reporting Database (Continued)**

To help ensure strong security over applications and the database for which data is stored, it is necessary for a strong password policy to be developed and implemented for MRDB and all applications within MARS. The likelihood of unauthorized processing, data alteration, and information leakage increases if applications and databases are not sufficiently secured. This compromises the integrity and confidentiality of the data that is processed through MARS and resides within the MRDB.

### Recommendation

We recommend FAC work with AMS to ensure optimal security features get incorporated in new versions of PD, BRASS, and MRDB to ensure each has optimal controls established for password security, such as expiration, preferably every 30 days; restriction on consecutive usage; and, a lockout feature following, at most, three (3) unsuccessful login attempts.

### Management's Response and Corrective Action Plan

*The planned 4.12 release of PD in October 2003 has error handling code contemplated to allow for minimum password length, forced password change, password re-use restrictions, and lockout after unsuccessful attempts. BRASS does not have these changes on a release schedule but is inquiring as to the level of effort, so they could be incorporated in future upgrades. MRDB is not a software application for which error handling must be incorporated in application code. It is no more than a set of Oracle tables representing extracts from other data sources managed through the Oracle Database Management System. While passwords are important to the MRDB, it is a "read-only" reporting system. We run Oracle routines periodically to search for weak passwords and ask users to change their passwords. We revoke user access after ample notification to change their MRDB Oracle passwords. MRDB is used for recurring reporting and to change passwords every 30 days will impose a hardship on the reporting process that doesn't meet the value test for the control. It is important to note at this juncture that BRASS, PD, and MRDB are not part of the Advantage Financial System, the Commonwealth's system of record for all financial information. The above recommendations for controls all currently exist in the Advantage Financial System.*

## FINANCIAL STATEMENT FINDINGS

***Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance***

### FINDING 02-FAC-6: The Finance And Administration Cabinet Should Work With The Governor's Office For Technology To Ensure The Security Log Report Is Generated, Recoverable, And Effectively Monitored

The FAC did not have controls in place that would ensure the security log report was generated, recoverable, and effective. MARS security violations are available for viewing within the security log report, FMP5G02, on-line through Document Direct or Remote Document Security (RDS). This report tracks security violations that occur in the Advantage Financial application. The most prevalent violation found within these reports is for error code *S304 (action not authorized for agency code) and *S302 (action not authorized). Per the Security Administrator, these error messages would be displayed for many reasons, such as:

- Entering the wrong agency code on a document;
- Failing to enter an agency code on a document; or
- Attempting to open a document/table entry for which the user does not have access.

This results in difficulty in determining whether or not the user simply made an error or was attempting to access something for which he/she did not have access. For this reason, the violation report is not reviewed on a regular basis. The report will be used for investigative purposes, if the need shall arise. For example, if an agency were to question the actions of a particular user.

Upon observation of the security log for selected run dates, we found that not all reports were available on-line through Document Direct or RDS. The security logs are missing from the end of January 2001 through the last part of August 2001. We were informed that it was likely the reports were not generated as a result of a migration being performed incorrectly. If the logs had been generated but are missing as a result of accidental or intentional destruction, the logs are not recoverable.

In addition, we found four (4) separate instances where a user had 18 security violations. There were two (2) different users associated with these violations on the same date. Though it appears that the document these users were attempting to process never made it to Advantage Financial, these instances were not brought to the Security Administrator's attention.

To help ensure strong security over applications, it is necessary the security log report be generated, recoverable, and effective. The likelihood of unauthorized processing and data change and information leakage increases if violations are not monitored. This compromises the integrity and confidentiality of the data processed through Advantage Financial.

## FINANCIAL STATEMENT FINDINGS

***Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance***

**FINDING 02-FAC-6: The Finance And Administration Cabinet Should Work With The Governor's Office For Technology To Ensure The Security Log Report Is Generated, Recoverable, And Effectively Monitored (Continued)**

### Recommendation

We recommend FAC work with the Governor's Office for Technology (GOT) to take the following steps to improve controls over the security log report:

- Implement a method of notification when the security log report is not generated.

- Implement a method of recovery in case there are missing reports as a result of accidental or intentional destruction.

- Develop filters for the security log so that it will be more useful for review and security notifications. If this cannot be done with the logging software, FAC should consider obtaining additional software to assist with the security log filtering and report development.

- Ensure the security log or resulting reports are adequately monitored and violations are investigated in a timely manner.

### Management's Response and Corrective Action Plan

*Any job (including reports) that abends in the nightly cycle shows up on the nightly note. Any job that abends at night can be re-run in the morning and posted to RDS provided the input files are not dynamic and don't change until the next cycle. Our previous issue referenced above wasn't that the reports didn't run, they just got out of the schedule to be posted to RDS when changes were made to the RDS environment. To solve the above problem and make the reports easier to use, we propose to place steps in the report job to append the daily detail lines to FINA.AFN1.SEQ.KR5G02 data set on the mainframe. This file can be FTPed and brought into MSAccess on a periodic basis allowing full database search functionality. At the end of each year the database will be archived to CD Rom and provided to the APA.*

## FINANCIAL STATEMENT FINDINGS

***Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance***

### FINDING 02-FAC-7: The Finance And Administration Cabinet Should Ensure All User Accounts On The Agency Servers Are Necessary

While performing interim vulnerability tests of FAC, we found several instances where unnecessary accounts were established on servers or for applications.

To examine the information provided by NetBIOS, we limited our review to 37 machines, including the Primary Domain Controller (PDC), Backup Domain Controllers, SQL servers, and NT servers. NetBIOS account information was received from seven (7) servers, including the PDC, within the FAC domain. We examined this information to search for disabled or unused user accounts. The PDC contained 32 disabled accounts. To determine possible unnecessary accounts, we used the criteria that the account was over the 31-day maximum password age established by FAC policy and had never logged onto the system. The PDC had 325 accounts that met this criterion. Further, while examining other FAC servers, we found the guest account on three (3) servers and two (2) user accounts on one (1) server met our criteria for potentially unnecessary accounts.

We attempted a remote logon to known applications using various combinations of default logon passwords. A review of all machines controlled by FAC revealed 85 machines with port 21 open and 67 machines with port 23 open. We were able to create a File Transfer Protocol (FTP) session through port 21 on 48 machines, or 56.5 percent, using the anonymous or guest logins. In addition, Telnet sessions could be established with no login or through the anonymous or guest default logins on 45 machines, or 67.2 percent, through port 23.

Intruders often use inactive accounts to break into a network. If a user account has not been used for a period of time, the account should be disabled until it is needed. This minimizes the possibility that an unauthorized user will use the account. An account should be deleted if it is not going to be reinstated. Further, default administrator, guest, and anonymous accounts in operating systems and applications are some of the first accounts that an intruder will attempt to use. Therefore, they should be assigned strong passwords or, if possible, renamed or removed immediately after installation.

#### Recommendation

We recommend FAC review accounts on all servers to determine which accounts had no password change within the last 31 days. These accounts should be evaluated to determine if they are still valid accounts required for a business-related purpose. If not, the accounts should be disabled or deleted as appropriate.

Further, FAC should ensure all machines with FTP or Telnet services running on them restrict access to default, anonymous, or guest logons.

## FINANCIAL STATEMENT FINDINGS

***Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance***

**FINDING 02-FAC-7: The Finance And Administration Cabinet Should Ensure All User Accounts On The Agency Servers Are Necessary (Continued)**

**Management's Response and Corrective Action Plan**

*Account Policies have been put in place, in addition to local administration account being modified every thirty days. Accounts over a certain time period are being reviewed for deletion.*

*FTP and Telnet ports are being reviewed and discussed as part of the FINANCE Cabinet discussions with GOT and the Firewall Solution they provide as a service to the Cabinet.*

*Internally any Services using well known Port numbers have been reviewed and services removed and/or disabled.*

## FINANCIAL STATEMENT FINDINGS

***Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance***

### FINDING 02-FAC-8: The Finance And Administration Cabinet Should Strengthen The Security Of Administrator Accounts

Vulnerability testing of FAC machines revealed several instances of lax security over administrator accounts, resulting in the potential of machines being vulnerable to intrusion.

We examined 37 FAC servers and found two (2) with blank local administrator account passwords. We were able to connect to and gain control of these servers. These vulnerabilities existed as of April 2002. However, these vulnerabilities were corrected by the end of the fiscal year. Also, the administrator account for seven (7) servers had not been renamed or disabled. Since the administrator cannot be locked out, if the account is not renamed, the server could be vulnerable to a potential intruder attempted to gain access by guessing the administrator password through a brute force attack.

Further, we examined all FAC controlled servers for specific applications that could be vulnerable and found four (4) machines with port 1433 open. One (1) server allowed the auditors to gain "Master" access through SQL using the default administrator logon. This type of access would provide an unauthorized user with complete access to the application. In addition, the user would be granted local system account rights to the server on which the application resides.

We found two (2) machines with port 80 open, allowing "Read/Write/All" access to remote administration of a switch through a default logon. This type of access would provide an unauthorized user rights to view and alter the switch configuration.

Administrator accounts are very powerful and can allow full access to the system. Therefore, these accounts should be scrutinized to ensure they are adequately secured. At a minimum, the passwords for these accounts should be changed from the system defaults. Further, some administrator accounts can be renamed to help obscure them from an unauthorized user's view.

#### Recommendation

We recommend FAC review all machines to ensure the local administrator accounts have been changed from the default naming conventions and require the use of a password. Further, all applications that might allow a user access to the system or to configuration settings should be reviewed to ensure default logons are not allowed.

## FINANCIAL STATEMENT FINDINGS

***Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance***

**FINDING 02-FAC-8: The Finance And Administration Cabinet Should Strengthen The Security Of Administrator Accounts (Continued)**

**Management's Response and Corrective Action Plan**

- *Local Administrator Accounts are being monitored now and will be changed on a regular basis.*

- *The SQL Server machine in question (using the default Administrator Password) was installed as a Demonstration of SQL Server. This machine has since been shut down and re-formatted.*

*Port 80 open allowing Read/Write/All access to remote administration of a switch through a default logon has been changed.*

## FINANCIAL STATEMENT FINDINGS

***Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance***

### FINDING 02-FAC-9: The Finance And Administration Cabinet Should Ensure All Open Ports On Agency Machines Have A Business-Related Purpose

During the interim security vulnerability assessment testing for servers controlled by FAC, we found several FAC servers with ports open that may not have a specific business-related purpose. Due to the large number of issues, the findings are grouped below by port number and application.

We tested machines based on the potential for misuse of port access. We originally tested 37 FAC servers, and then expanded testing to all FAC controlled machines to examine ports 80, 443, and 8000.

Port 7 – Echo and Port 19 - Chargen
Three (3) servers had both ports 7 and 19 open. These ports are not necessary for the function of the server and could potentially be used to perpetuate a Denial of Service (DoS) attack.

Port 70 - Gopher
Two (2) servers had port 70 open. This port supports the obsolete Gopher application, which is no longer needed. Despite some efforts to revive Gopher, virtually all Gopher servers are no longer active. Therefore, it is likely that this port is not needed for a business purpose.

Port 80 – Hypertext Transfer Protocol (HTTP)
Port 80 was open on 47 machines that would not display the website. When no default page or restricted logon is required, normally this means that no application/web service is running at the port. Additionally, configuration information for printers or print servers was provided by 49 websites. This situation allows too much access to an unauthorized or anonymous user. Finally, using one (1) vulnerability assessment tool we determined that anonymous viewing restrictions were needed for several well-known web service directories present on one (1) server. We were able to access four (4) of these directories and view the pages without restriction.

Port 443 – Hypertext Transfer Protocol over Secure Socket Layer (HTTPS)
Nine (9) servers were found with port 443 open but would not display a website. When no default page or restricted logon is required, normally this means that no application/web service is running at the port.

Port 6667 – Internet Relay Chat
Five (5) servers in the FAC domain were discovered with port 6667 open. This port can be used for several serious exploitations, such as DoS attacks, Trojan horse attacks, and downloading of illegal files. This port could be useful to a hacker and should only be used for a necessary business-related application.

## FINANCIAL STATEMENT FINDINGS

***Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance***

**FINDING 02-FAC-9: The Finance And Administration Cabinet Should Ensure All Open Ports On Agency Machines Have A Business-Related Purpose (Continued)**

Port 8000 – HTTP
Twenty-six (26) servers owned by FAC were discovered that had port 8000 open. Seventeen (17) of these servers do not display the website. These do not appear to have an application/web service running on them. The remaining nine (9) servers revealed configuration information for printers/print servers. This situation allows too much access to an unauthorized user.

Other Ports
Four (4) servers had ports open that do not appear to specifically relate to known business applications. FAC should review all open ports on servers to ensure that all have a valid business-related purpose.

The existence of open ports is an invitation for intruders to enter your system. To minimize the risk of unauthorized access to a machine, only necessary, business-related ports should be open, and all applications residing at these ports should be secured to the extent possible.

### Recommendation

We recommend FAC perform a review of all open ports on the servers discussed in this comment. If there is not a specific, business-related purpose requiring a port to be open, then that port should be closed. Further, we recommend FAC begin a periodic review of open ports on all machines owned by the agency to ensure necessity.

### Management's Response and Corrective Action Plan

*FINANCE is currently working with GOT Firewall support personnel to configure a Firewall solution to further protect the FINANCE Cabinet Data and resources from outside attack.*

## FINANCIAL STATEMENT FINDINGS

***Other Matters Relating to Internal Controls and/or Instances of Noncompliance:***

### FINDING 02-FAC-10: The Finance And Administration Cabinet Should Improve Investment Related Closing Package Forms And Instructions

FAC'S CAFR team prepares the Cash and Investments note (Note 5). In reviewing the Note 5 related closing package forms for each component unit, we noted:

1) Few instructions are provided on the AFR 80 Reconciliation of Cash and Investments, AFR 121 Statement of Activities, AFR 126(a) Cash and Investments not Held by the State Treasury, and AFR 126(b) Amount of Cash and Investments Held by the State Treasury forms regarding their preparation. As a result, these forms were not prepared consistently and many component units filled them out incorrectly. Some component units even failed to submit forms.

   Without proper instructions on the AFR 80, 121, 126(a), and 126(b) forms, component units may not prepare forms correctly or in the same manner across the Commonwealth. For example, the Combining Statement of Activities on page 178 of the CAFR reported interest income in the amount of $4,505,000. This amount was taken directly from each component unit's AFR 121. However, these component units did not prepare their AFR 121 form uniformly, resulting in $10,949,505 of interest income being misclassified.

   Adding clear instructions to the AFR forms will allow the financial statements to be prepared consistently and uniformly throughout the Commonwealth, which will further improve the quality of the information being reported.

2) Accounting terminology (such as carrying value, fair value, and market value) was not used consistently, which could create confusion.

   If accounting terminology is not used consistently, then this could lead to confusion over what information is actually needed on the forms, resulting in incorrect information being reported. Since these forms are used when preparing financial statements, if they are prepared incorrectly, then the information in the Commonwealth's financial statements could be materially misstated.

   Accounting terminology must be used consistently on the AFR forms for the forms to be prepared correctly and uniformly throughout the Commonwealth.

## FINANCIAL STATEMENT FINDINGS

***Other Matters Relating to Internal Controls and/or Instances of Noncompliance:***

**FINDING 02-FAC-10: The Finance and Administration Cabinet Should Improve Investment Related Closing Package Forms And Instructions (Continued)**

Also, according to paragraph 6 of GASB 31 *Accounting and Financial Reporting for Certain Investments and for External Investment Pools*, the term "market value" was replaced by "fair value."

> This Statement amends Statement 2 and GASB Statements No. 3, Deposits with Financial Institutions, Investments (including Repurchase Agreements), and Reverse Repurchase Agreements, and No. 28, Accounting and Financial Reporting for Securities Lending Transactions, by replacing the previously used term market value with the term fair value.

The forms have note been updated since they still use the term "market value."

3) Many of the component units prepared their forms using the carrying value (book value) of cash and investments in the State Investment Pool when they should have used fair value.

If the carrying value of cash and investments is reported on the AFR forms instead of fair value, then the financial statements will not be prepared in accordance with GAAP. In addition, the financial statements will not accurately present the financial position of the component unit, resulting in assets that are either understated or overstated, depending upon market conditions.

Fair value of the State Investment Pool cash/investments (instead of carrying value) should be reported on the Statement of Net Assets according to paragraph 7 of GASB 31 Accounting and Financial Reporting for Certain Investments and for External Investment Pools:

> Governmental entities, including governmental external investment pools, should report investments at fair value in the balance sheet. Fair value is the amount at which an investment could be exchanged in a current transaction between willing parties, other than in a forced or liquidation sale . . ..

**Recommendation**

We recommend that terminology and instructions on the AFR 126(a), 126(b) and AFR 80 forms be updated to provide clear instructions and consistent terminology so that component units can prepare these forms correctly and uniformly throughout the state. Also, we recommend FAC ensure component units use fair value instead of carrying value in their financial statements. Changes to the AFR forms/instructions and the confirmation database could provide the component units and their auditors with a clearer understanding of how to correctly complete the AFR forms.

## FINANCIAL STATEMENT FINDINGS

***Other Matters Relating to Internal Controls and/or Instances of Noncompliance:***

**FINDING 02-FAC-10: The Finance and Administration Cabinet Should Improve Investment Related Closing Package Forms And Instructions (Continued)**

**Management's Response and Corrective Action Plan**

*We agree with the recommendations and have redesigned the AFR forms and the confirmation report. The redesigned forms stress the requirement to report at fair value. The more consistent terminology should provide component units with a clearer understanding of how to more accurately complete the AFR forms. The new confirmation report, as recommended, will now report long and short term carrying value and fair value. These improvements should result in more consistent reporting.*

## FINANCIAL STATEMENT FINDINGS

***Other Matters Relating to Internal Controls and/or Instances of Noncompliance:***

### FINDING 02-FAC-11: The Office Of Financial Management Should Ensure Adequate And Consistent Reconciliations

During our review of OFM's internal controls, we noted some weaknesses in the reconciliation area:

- OFM lacked consistent documentation of reconciliations of CAMRA to Bank of New York, and reconciliations were performed infrequently. The last reconciliation maintained before the switch to State Street, as custodian bank, was for December 2001. Also, during the transition from the old custodian bank (Bank of New York) to the new one (State Street), no reconciliations to Bank of New York were documented by OFM or Farmers Bank.

- The reconciliations for FY 02 did not consistently provide adequate explanations of differences and/or document follow up on the differences.

When adequate reconciliations are not performed on a consistent basis, errors can occur in reporting financial information.

Good internal controls dictate that adequate reconciliations be performed on a consistent basis to ensure the accurate reporting of financial information.

#### Recommendation

We recommend OFM maintain consistent reconciliations, with adequate documentation of differences and/or documentation of follow up on the differences. Proper reconciliations should be performed on a consistent basis between CAMRA and the custodian bank, and reconciliations should be performed by someone other than the staff member recording the financial information. Reconciliations should be documented and provide clear explanations of differences and document follow up of differences noted. The reconciliations for FY 03, performed weekly, were very detailed and follow up was adequate and well documented. OFM should continue to use this reconciliation process. Reconciliations should be formally reviewed by management or the internal auditor, and documented by a signature or initials.

We are aware that OFM is completing a policies and procedures manual. OFM should distribute copies of the policies and procedures manual, and meet with all staff members to discuss their duties when the manual is complete.

## FINANCIAL STATEMENT FINDINGS

***Other Matters Relating to Internal Controls and/or Instances of Noncompliance:***

**FINDING 02-FAC-11: The Office Of Financial Management Should Ensure Adequate And Consistent Reconciliations (Continued)**

**Management's Response and Corrective Action Plan**

*OFM has already set procedures in place that will insure that reconciliations are done timely. The APA noted above that reconciliations are now timely and adequately documented. A communication breakdown with Farmer's Bank caused the gap in balancing of portfolios. Historically Farmer's reconciled to Bank of New York. With the moving of custody to State Street Farmer's felt the Commonwealth had access to the same information as they did. With the limitation of staff size at OFM it is difficult to separate entry of trades from reconciling of portfolios. We now have a solution where whichever individual enters trades into a database does not reconcile that database.*

## FINANCIAL STATEMENT FINDINGS

***Other Matters Relating to Internal Controls and/or Instances of Noncompliance:***

### FINDING 02-FAC-12: The Office Of Financial Management Should Ensure Trading Limits Are Monitored

OFM personnel executing investment trades are not always adequately monitored for adherence to individual trading limits as established by the State Investment Commission.

Individual trading limits were exceeded for two (2) of the 45 investment purchase transactions tested. There was no documentation showing the necessity or approval to exceed established limits.

If individual trading limits are not adhered to or monitored:

- holding limits for specific security types as required by 200 KAR 14:011, 081, and 091 may be exceeded;
- investment strategies may not be properly followed and goals may not be reached.

In the September 30, 1998 State Investment Commission Meeting, the Committee limited three (3) OFM employees to investing in only certain securities for specific amounts.

#### Recommendation

We recommend that OFM:

- adequately monitor for adherence to trading limits,
- document the necessity and approval to exceed those limits, and
- increase trading limits to more practical levels, if necessary.

#### Management's Response and Corrective Action Plan

*The Office of Financial Management (OFM) agrees that it is important to adhere to trading limits allowed by the State Investment Commission. OFM has added additional monitoring of trades to preclude limit issues in the future. OFM also had the State Investment Commission update trading limits to more appropriate levels.*

## FINANCIAL STATEMENT FINDINGS

***Other Matters Relating to Internal Controls and/or Instances of Noncompliance:***

### FINDING 02-FAC-13: The Office Of Financial Management Should Ensure Adequate Segregation of Duties

During our review of OFM's internal controls, we noted the following weaknesses in segregation of duties:

- One (1) staff member enters trade information in MARS and CAMRA. The same staff member reconciles these two systems.

- One (1) staff member reconciled CAMRA to Bank of New York (the old custodian bank); however, while the staff member was gone on leave for three (3) months no reconciliations were performed between CAMRA and Bank of New York.

When one (1) staff member records information and reconciles it, without a separate review, errors can occur without being discovered.

Good internal controls dictate that segregation of duties must be adequate for recording, maintaining, and reporting financial information.

**Recommendation**

1. We are aware that OFM is completing a policies and procedures manual. OFM should distribute copies of the policies and procedures manual, and meet with all staff members to discuss their duties when the manual is complete.

2. One (1) staff member should enter information into CAMRA, and/or MARS. A staff member who does not record information in CAMRA or MARS should reconcile the two (2) systems. The internal auditor or a manager should review all reconciliations and sign/initial the reconciliations.

**Management Response and Corrective Action Plan**

*This has been a recurring issue since the inception of MARS. It is difficult to separate the investing, accounting and database management with the size of staff OFM has. The addition of two part-time employees has added to the ability of separating tasks. OFM now has one individual entering data into MARS, another one into CAMRA and a third individual reconciling the two.*

## FINANCIAL STATEMENT FINDINGS

***Other Matters Relating to Internal Controls and/or Instances of Noncompliance:***

### FINDING 02-FAC-14: The Finance And Administration Cabinet Should Continue To Strengthen The Procedures For Recording Contingent Liabilities

During our review of contingent liabilities and the accounting methods used to record those amounts in the financial statements, we discovered that the FAC Reporting Team did not use consistent methods for reporting this activity. Contingent liability information is requested from each agency via the "Closing Package". The instructions for reporting contingent liabilities dictate they should be "divided into the following categories: a) remote – less than 50% chance of occurrence, b) possible – 50%-75% chance of occurrence, and c) probable – greater than 75% chance of occurrence. Only probable liabilities for which the loss is reasonably estimable should be included as contingent liabilities."

Our testing required review of all "Closing Packages" relating to contingent liabilities. We noted that not all agencies followed the instructions for reporting this information – several agencies did not break out the information into the "remote, possible, or probable" categories as required. Based on our review of the language used by the agencies in their "Closing Package" we determined that an adjustment to the financial statements was necessary.

#### Recommendation

We recommend that the FAC Reporting Team review the information presented by the agencies and require they comply with the "Closing Package" instructions. Consistent treatment should be applied to all the state's agencies for information presented in the financial statements.

#### Management's Response and Corrective Action Plan

*We concur. The FAC reporting team is revising the instructions to the Closing Package to facilitate in the gathering of this information. We will review each closing package submitted for compliance with instructions and we will ensure that each agency's information is consistently reported.*

## FINANCIAL STATEMENT FINDINGS

***Other Matters Relating to Internal Controls and/or Instances of Noncompliance:***

### FINDING 02-FAC-15: The Finance And Administration Cabinet Should Closely Examine The Closing Packages Prepared By The Agencies For Accurate Completion

As part of our audit of the Commonwealth of Kentucky's financial statements, we became aware of opportunities for strengthening the reporting function of closing package information submitted by state agencies, as well as strengthening operating efficiency.

Each fiscal year, the Division of Statewide Accounting Services schedules closing package training. State agencies are asked to send staff responsible for the preparation of the financial information to these training sessions for instructions on the various closing package forms.

We noted several problems during our FY 02 audit that we believe may have resulted from a lack of clear instructions, training, and/or follow-up with the agencies preparing closing packages. We noted problems and prepared either written or verbal comments relating to these areas in our audits of the Cabinet for Health Services, the Cabinet for Workforce Development, the Office of Financial Management, and Finance and Administration Cabinet (Fixed Assets).

Although current instructions for closing package completion are fairly comprehensive, they would be enhanced if clear, succinct instructions, using consistent accounting terminology, were provided. Instructions should be easy to follow for each form, and terms should be consistent throughout the instructions. If provided, it is believed that it would be easier to achieve consistency when closing package forms are completed.

#### Recommendation

We recommend the following be considered:

- Consistent use and accurate meaning of terminology
- Review and update closing package forms to achieve reporting consistency
- Development of a comprehensive and expanded training program for the correct preparation of the closing package forms
- Follow-up with agencies, including random site visits, to provide assistance, answer questions, and ensure that the forms are properly completed and reviewed by appropriate staff

## FINANCIAL STATEMENT FINDINGS

***Other Matters Relating to Internal Controls and/or Instances of Noncompliance:***

**FINDING 02-FAC-15: The Finance And Administration Cabinet Should Closely Examine The Closing Packages Prepared By The Agencies For Accurate Completion (Continued)**

**Management's Response and Corrective Action Plan**

*We will review the closing package for consistent use and accurate meaning of terminology and update the forms to achieve reporting consistency. Each year the FRT provides closing package training. We will send each agency a memo strongly encouraging participation in the training sessions. In addition, we will try to be more active in providing hands on assistance in the preparation of the closing package by offering workshops that will allow agency personnel to ask questions and receive assistance.*

## FINANCIAL STATEMENT FINDINGS

***Other Matters Relating to Internal Controls and/or Instances of Noncompliance:***

### FINDING 02-FAC-16: The Finance And Administration Cabinet Should Develop Formal Procedures For System Assurance Efforts Concerning The Financial Analysis System

As stated in the previous audit for FY 01, it was noted that there are no formal procedures in place for assuring the completeness or reliability of Financial Analysis System (FAS) data. FAS is a client/server reporting system that is accessed via the Internet and permits system users to analyze MARS financial data with minimal effort and expertise.

The primary source of data for this system is from the MRDB, a component of MARS. Therefore, the Office of Technology Services (OTS) makes the assumption that the data is accurate. OTS is dependent on system users to notify the division when system errors or inaccurate data occur that should then be investigated. Often the nature of the discrepancy is not readily determined.

The FAS data is completely rebuilt each night and a nightly cycle report is generated the following morning for review. This nightly cycle report lists the filename, file size and date of file creation. This report is manually examined only to determine that information appears reasonable. If for some reason the data does not appear complete, since OTS performs a complete rebuild each night of FAS, the next nightly cycle is expected to correct any problems. No other formal procedures are performed to assure FAS data and/or system totals are accurately downloaded for reporting purposes.

Ultimately, OTS is responsible for the support of the application and should ensure the accuracy of data. When discrepancies are noted, OTS personnel should determine the reason and best method of correcting the discrepancy. Ideally, once problems have been corrected, comparison reports should be reproduced to ensure that the problem has been corrected and that there are no further problems. There are currently no written procedures in place concerning the use of management reports to assure FAS data accuracy.

Formalized procedures and standards should be implemented for the daily FAS system assurance procedures, and should include report comparisons to MRDB. Formalized procedures should also include descriptions of the OTS employee's processes and the steps taken to resolve errors that are noted within these system assurance efforts. Further, reconciliations should be performed daily to ensure that totals agree with reports from MRDB. Formalized system assurance procedures provide continuity for procedure implementation and illustrate management's concern for strong data integrity within the system.

## FINANCIAL STATEMENT FINDINGS

***Other Matters Relating to Internal Controls and/or Instances of Noncompliance:***

**FINDING 02-FAC-16: The Finance And Administration Cabinet Should Develop Formal Procedures For System Assurance Efforts Concerning The Financial Analysis System (Continued)**

### Recommendation

We recommend that OTS develop detailed written procedures documenting the processes to be followed for the creation and review of the daily and monthly system assurance reports between the FAS and the MRDB, and for the correction of errors discovered through review of these reports. Further, these procedures should be distributed to all employees that are involved with the FAS system assurance task.

### Management's Response and Corrective Action Plan

*OTS Proposed Solution: System assurance reporting can be automated/computerized to the extent of e-mailing recipients of failing conditions within software output production. As FAS.V2 is developed, checks for data integrity are designed to be built in. However, this step cannot take place until a dissection of documented Commonwealth business-rules takes place. Once business rules and data needs are recorded, data integrity can be ensured through a series of check-sums and random text identification measures. This solution is co-incident to FAS.V2 design and creation; when FAS.V2 is turned on this solution is scheduled to be in place.*

## FINANCIAL STATEMENT FINDINGS

***Other Matters Relating to Internal Controls and/or Instances of Noncompliance:***

### FINDING 02-FAC-17: The Finance And Administration Cabinet Should Continue To Work In Conjunction With The Governor's Office For Technology To Implement Logging And Audit Features Within Procurement Desktop

As was noted in the previous two audits, the PD system lacks security features that would identify users who make changes to the PD database. Currently in PD, logging is still not performed for user-initiated transactions or security-related access attempts. In this situation, users who make changes to the data or attempt unauthorized accesses are not traceable and could cause system hardships if inappropriate or unauthorized changes are made to the PD database.

Improvements were noted with the release of Version 4.8 in which document approvals are recorded and changes to some PD databases may be observed, (i.e., vendor table). Additional progress was made with the release of PD Version 4.9 in May 2002 as well. These improvements included the synchronization of the time and date stamps to the server time, and the Catalog Master Agreements will require a modification for changes that are documented in the tables. It was also noted that GOT logs failed access attempts for general PD users and successful attempts by AMS staff that have update access to the data outside of the application.

While progress has been made, weaknesses still exist that should be addressed. Currently, only high-level database IDs are locked out after three failed access attempts. It was also noted that PD users are allowed to log into the system using IDs other than their own. Further, database administrators review the PD logs weekly, but only for activity on the high level IDs and for structure changes.

As was reported last year, FAC and GOT began working with AMS to fully incorporate procurement data from PD into MRDB with FAC specifically requiring the logging of changes and failed login attempts for PD in September 2001. It is proposed that the Controller's Office, along with the Division of Material and Procurement Services and GOT, will take over the PD MRDB project. Information is still being gathered before the development phase of this project is scheduled. Finance is in the process of determining exactly what information should be logged and who will be in charge of this task.

Without sufficient logging and auditing features, a system is vulnerable to probes, scans, or attacks that could be perpetrated on the system for extended periods of time without proper intrusion detection and incident response by the owner of the data or programs.

## FINANCIAL STATEMENT FINDINGS

***Other Matters Relating to Internal Controls and/or Instances of Noncompliance:***

**FINDING 02-FAC-17: The Finance And Administration Cabinet Should Continue To Work In Conjunction With The Governor's Office For Technology To Implement Logging And Audit Features Within Procurement Desktop (Continued)**

### Recommendation

Our recommendation includes the following suggestions:

- FAC and GOT should continue to ensure, through the implementation plan in progress with AMS, that logging and auditing features are designed appropriately and fully implemented for the PD Oracle environment to provide sufficient audit trails of database alterations or security violations.

- A lock out feature should be part of the security settings for the PD system. It is recommended that user IDs be locked after three failed login attempts.

- Users should only be allowed to log into the PD system with their own personal user ID and password. Sharing of IDs and passwords is a security violation and increases the risk of inappropriate or unauthorized changes to the system, and the inability to specifically identify the user initiating transactions.

- The resulting PD log(s) should be appropriately reviewed to ensure that no unauthorized access attempts or data changes are made.

### Management's Response and Corrective Action Plan

*PD Oracle database logging is captured for all database changes. The "archive file" (ARCHLOG_P2: assigned file name) can be researched using an Oracle tool "Log Miner". These files are quite large and are not currently kept beyond the previous day. We are proposing that these log files be written to CD-ROM or tape and kept for a period of 1 year. While logging is a good idea, it is worthy of note that the Advantage Financial System is the system of record where all recommended activity already occurs. Logging activity within the application is restricted to approvals, vendor changes, and User ID changes. Extensive logging within the application has a profound impact on system performance, and will be used sparingly. Failed access attempts and high-level database privilege activity are currently logged in DBASUPP1: PDSKP2_AUDIT_SESSION that can be viewed using MS Access. DBA's currently review these tables weekly, and we propose that a quarterly review be done by the MARS Security Administrator.*

*PD Password length, forced change, re-use, and lockout features are covered in G-21 G (I-IV). It is currently policy to prohibit the sharing of passwords an example of language promoting that policy may observed in the Sept 2001 MARS UPDATE: MARS BRASS UPDATE: "Reminder: Protecting Your MARS PASSWORD"*

## FINANCIAL STATEMENT FINDINGS

***Other Matters Relating to Internal Controls and/or Instances of Noncompliance:***

### FINDING 02-FAC-18: The Finance And Administration Cabinet Should Consistently Apply Established Program Modification Control Procedures For The Financial Analysis System

As indicated in the previous audit, FAC does not have formal procedures in place to ensure the authorization of program modifications to FAS. During the audit period, FAC did not maintain a log or monitor requests made for FAS program changes. All program modifications were made without formal documentation by the system developer.

Unlike other information systems, FAC does not rely on GOT to complete program modifications requested for FAS. Staff in the Office of Technology Services makes all program changes. These same employees are responsible for testing and placing FAS programs into production.

Ideally, program change requests should be documented and procedures should be in place to track the progress of requests. Program modification procedures should include system-testing efforts to ensure program modifications meets requirements. Testing facilities assure that any problems are identified and re-tested before they are placed into the production environment. There should also be adequate documentation of user acceptance and authorization prior to placing modified programs into production. Additionally there should be adequate segregation of duties between programmer and librarian functions. Programmers should not have ready access to production source code.

#### Recommendation

We recommend that FAC develop and distribute specific polices and procedures for program changes to FAS. OTS should ensure personnel are aware of and trained on the proper procedures for requesting, authorizing, monitoring, and moving into production any changes for FAS programs. Documentation of FAS program change requests, request status, and evidence of proper authorization for changes should be maintained as an audit trail.

#### Management's Response and Corrective Action Plan

*OTS Proposed Solution: This documentation is scheduled for finalization at the time of FAS.V2 deployment. It is not needed before then, as no system changes are to be allowed until FAS.V2 is complete/deployed (other than those specifically listed in this document). Once FAS.V2 is in use, FAS.V2 users will be instructed through an e-mailing of the only acceptable procedure for initiating a change-order for the FAS.V2 system. At the current time, this procedure is proposed to include:*

## FINANCIAL STATEMENT FINDINGS

***Other Matters Relating to Internal Controls and/or Instances of Noncompliance:***

**FINDING 02-FAC-18: The Finance And Administration Cabinet Should Consistently Apply Established Program Modification Control Procedures For The Financial Analysis System (Continued)**

**Management's Response and Corrective Action Plan (Continued)**

1) *The FAS.V2 user accesses the OTS web site for a form that must be completed and sent to OTS for review. This form will be stored in a database. This form will require the signatures of the originator of the request, the originator's supervisor, and the Secretary of the originator's Cabinet.*

2) *OTS actions taken will be recorded in this same database (high-level, as a disposition). At the same time, internal OTS documentation will be initiated and recorded. As an example:*
    *1) What is the actual (high level) change being requested?*
    *2) Why are we making this change (what is the benefit)?*
    *3) Who would this change affect?*
        *a) How does this change affect the System Administrator?*
        *b) How does change affect procedures at OTS?*
        *c) How does change affect procedures at GOT?*
        *d) How does this change affect other FAS users?*
3) *What does the requested change affect?*
    *( ) FAS.V2 Design*
    *( ) Hardware*
        *( ) Users*
        *( ) MRDB*
        *( ) Web Server*
        *( ) Other*
    *( ) Software*
        *( ) Extract Transformation Loaders*
        *( ) FAS-User*
        *( ) Other*
    *( ) Operating System*
        *( ) Users*
        *( ) MRDB*
        *( ) Web Server*
        *( ) Other*
        *a) How does this change affect the indicated system?*
4) *Where would these changes take place?*
        *( ) OTS*
        *( ) GOT*
        *( ) Other*
        *a) How (what languages/computer resources are involved)?*
5) *What is the time-frame (schedule) for this change?*

## FINANCIAL STATEMENT FINDINGS

***Other Matters Relating to Internal Controls and/or Instances of Noncompliance:***

**FINDING 02-FAC-18: The Finance And Administration Cabinet Should Consistently Apply Established Program Modification Control Procedures For The Financial Analysis System (Continued)**

**Management's Response and Corrective Action Plan (Continued)**

*Once request has been managerially authorized for further action, the request is assigned to programming staff for further review and refinement. At the time of authorization/rejection becoming final (either way), the originator of the request is contacted as to its disposition. If the decision is made to progress, the request is scheduled for programmer action. Once the approved request (remember this may not be exactly what the originator specified; it may have been changed during the approval process) has been assigned to programming staff, request parameters should be loaded into MS-Project for monitoring project/request progress. Project progression will be recorded daily in MS-Project until the project/request is programmatically complete. Once a change is deemed programmatically complete, it should be made available (in a test environment) to the user for testing purposes. Once the request originator accepts the change, a sign-off form must be completed indicating originator approval.*

*This sign-off sheet signed by the programming staff involved, and OTS management shows the task as complete. Once the change is deployed in FAS, it will undergo a minimum of one full calendar month (during the next entire full month) Commonwealth review period. During this time, issues may arise from other Cabinets/FAS users with respect to this change that may require further modification (for operational stability only; enhancements must go through this same process) or possibly deletion.*

## FINANCIAL STATEMENT FINDINGS

***Other Matters Relating to Internal Controls and/or Instances of Noncompliance:***

### FINDING 02-FAC-19: The Finance And Administration Cabinet Should Improve Logical Security Measures Over The Financial Analysis System

FAC facilitates security access authority to the FAS through the OTS. As noted in the previous audit for FY 01, OTS has not adequately established proper logical security measures for this reporting system.

Originally OTS administered the security for FAS access centrally. Now, FAS security administrators are established by OTS based on information provided through the Agency Implementation Leads (AILs) or their designee. Ideally, these security administrators would issue user IDs and passwords in the effort to control and monitor logical access. It should be noted that FAS does contain some data that is highly sensitive such as personnel data including personnel profile information like salaries and leave balances. The issues are summarized below to specifically identify security weaknesses noted within the FAS system:

- FAS system does not maintain an audit feature to track id assignments and/or user profile changes. Formal documentation did not exist on a consistent basis to support the FAS access provided to users.

- Our review revealed that due to recent decentralization of FAS access administration throughout the various state agencies, 60 users have security administrator level access to update user profiles. There are currently approximately 1075 FAS users. This appears to be an excessive number of employees with the ability to update user security profiles. It would be more cost efficient to control FAS access centrally.

- Formal policies and procedures have not been developed and distributed to security administrators concerning FAS access security controls. Security Administrators may not fully understand their responsibilities to obtain and retain well-documented access authorization forms or email, which would support access granted and/or the access removed.

- The FAS profile update capability does not limit the FAS security administrators from providing users more access than needed to perform the work for their functional area within their agency. Therefore, a FAS security administrator could issue user privileges to all agency data, when a valid user request may not require that level of access.

- Each user password is readily visible in clear text by all security administrators on the security maintenance screen. This includes the passwords for other security administrators' accounts.

## FINANCIAL STATEMENT FINDINGS

***Other Matters Relating to Internal Controls and/or Instances of Noncompliance:***

**FINDING 02-FAC-19: The Finance And Administration Cabinet Should Improve Logical Security Measures Over The Financial Analysis System (Continued)**

- FAS does not force an initial password change for new users nor does the system require password changes on a frequent basis.

- Training has been provided to the various FAS security administrators, but adequate training was not provided to agency supervisors responsible for requesting access for their employees. This lack of training may cause supervisors to be unaware of the consequences of profile changes they might request or authorize.

System security should be administered in such a way as to ensure proper segregation of duties, and access to FAC data should be granted on an as needed basis. Formal procedures should be established for system access controls to ensure security is not compromised. Formal documentation should be maintained to support authorization for the access actually granted FAS users. Centralized management of logical security efforts is generally viewed as a more efficient means of security administration, and will likely be more cost effective. Users with the capability to add or change user access should be limited to a few key personnel. Passwords should not be visible in clear text to users or system administrators. Supervisors and managers requesting changes to user security profiles should be properly trained.

**Recommendation**

We recommend FAC take the following steps to improve the logical security administration function for FAS:

- OTS should establish polices and procedures for improving the logical security effort by FAS security administrators. Formal procedures should be implemented requiring submission and maintenance of documentation for FAS access requests and authorizations.

- FAC should consider re-instating centralized access control responsibility for FAS within the OTS.

- System audit features should be activated to record system ID assignments and/or user changes.

- User passwords should be shadowed, suppressed, or encrypted on the security maintenance screen to prevent unauthorized FAS access. Applicable system password files should also be encrypted.

- Adequate training should be provided to supervisors and managers responsible for requesting system access to ensure they understand the consequences of profile changes requested.

## FINANCIAL STATEMENT FINDINGS

***Other Matters Relating to Internal Controls and/or Instances of Noncompliance:***

**FINDING 02-FAC-19: The Finance And Administration Cabinet Should Improve Logical Security Measures Over The Financial Analysis System (Continued)**

**Management's Response and Corrective Action Plan**

*OTS Proposed Solution: The concept of withdrawing FAS access administration to OTS central office is currently being reviewed. If access security is administered from OTS central office, this concern is moot (regarding FAS administrators). If the decision is made not to handle access security centrally, a procedure will be defined at that time, but will include as a minimum:*

*Persons needing access would direct their browser to the OTS web-page and complete a form requesting access. This form must be also signed by the requestor's supervisor and the requestor's Cabinet Secretary.*

*Supervisory signatures are required to indicate that management within the Commonwealth is aware of changes being made to the FAS system regarding specific user access. A System Administrator Manual is scheduled to be produced/finalized at the conclusion of FAS.V2 development and deployment for handling OTS Central Office procedures regarding FAS security access.*

***Auditor's Recommendation:*** *FAC should consider re-instating centralized access control responsibility for FAS within the Office of Technology Services.*

***OTS Proposed Solution:*** *A stated previously, this recommendation is currently under review.*

***Auditor's Recommendation:*** *System audit features should be activated to record system ID assignments and/or user changes.*

***OTS Proposed Solution:*** *This suggestion is scheduled to be incorporated in the design changes for FAS.V2 (the FAS re-write).*

***Auditor's Recommendation:*** *User passwords should be shadowed, suppressed, or encrypted on the security maintenance screen to prevent unauthorized FAS access. Applicable system password files should also be encrypted.*

***OTS Proposed Solution:*** *This suggestion is scheduled to be incorporated in the design changes for FAS.V2 (the FAS re-write). A further breakdown is suggested; both the original auditor's suggestion and then the prospect of having the actual password file encrypted for added security (thereby negating easy access from other systems such as MS-Access, etc).*

## FINANCIAL STATEMENT FINDINGS

***Other Matters Relating to Internal Controls and/or Instances of Noncompliance:***

**FINDING 02-FAC-19: The Finance And Administration Cabinet Should Improve Logical Security Measures Over The Financial Analysis System (Continued)**

**Management's Response and Corrective Action Plan (Continued)**

***Auditor's Recommendation:*** *Adequate training should be provided to supervisors and managers responsible for requesting system access to ensure they understand the consequences of profile changes requested.*

***OTS Proposed Solution:*** *Once FAS.V2 is in place, this training will be developed and put into place for those affected. Office of the Auditor of Public Accounts will be contacted regarding this training.*

## FINANCIAL STATEMENT FINDINGS

***Other Matters Relating to Internal Controls and/or Instances of Noncompliance:***

### FINDING 02-FAC-20: The Finance And Administration Cabinet Should Develop And Implement Formal Written Policies And Procedures Concerning Security Of The Financial Analysis System

As noted in the previous audit for FY 01, FAC did not develop and implement formal written security policies and procedures identifying management and user responsibilities concerning security of the FAS. We recognize that FAC is currently in transition with changes being made to the infrastructure and management of FAS. However, these formal policies had not been developed as of the date of our follow up with this comment.

FAS is a client/server reporting system that is accessed via the Internet and permits system users to analyze MARS financial data with minimal effort and expertise. There are approximately 1075 current users of FAS and no formal policies have been developed concerning procedures for ensuring proper access to this reporting system. A draft policy has been prepared for use by the Customer Resource Center and has served as the primary reference for recent training of FAS Security Administrators at the agency level. If an individual requests access to FAS, they are directed to their respective FAS Security Administrator. Therefore, FAC should not only develop and implement policies concerning their central level oversight for FAS security but also disseminate policies to be followed by agency level FAS Security Administrators.

Failure to adequately document and communicate security policies could lead to a lack of understanding by management and users resulting in a failure to comply with security policy. Non-compliance with security policies may also lead to unauthorized data or program modification, destruction of assets, and interruption of services. Further, lack of documented disciplinary action procedures may allow for inconsistent treatment of security violators.

For security to be effectively implemented and maintained, detailed written policies and procedures must be developed. These procedures provide the security framework used to educate management and users of their security responsibilities. Further, formalized security policies provide continuity for policy implementation and illustrate management's concern for strong computer system and data resource security.

#### Recommendation

We recommend FAC develop and implement security policies and procedures that will help ensure the security of access to the FAS. This effort should include policies to be disseminated out to the FAS Security Administrators at the agency level.

## FINANCIAL STATEMENT FINDINGS

***Other Matters Relating to Internal Controls and/or Instances of Noncompliance:***

**FINDING 02-FAC-20: The Finance And Administration Cabinet Should Develop And Implement Formal Written Policies And Procedures Concerning Security Of The Financial Analysis System (Continued)**

**Management's Response and Corrective Action Plan**

*OTS Proposed Solution: The concept of centralizing FAS security access is under review by OTS management. Upon final decision, policies and procedures will be drawn up for those affected.*

*If FAS security access is to be centralized at OTS (through the OTS security officer), persons needing access would direct their browser to the OTS web-page and complete a form requesting access. This form must be also signed by the requestor's supervisor and the requestor's Cabinet Secretary. Then forwarded to OTS for their review and action. Supervisory signatures are required to indicate that management within the Commonwealth is aware of changes being made to the FAS system regarding specific user access.*

## FINANCIAL STATEMENT FINDINGS

***Other Matters Relating to Internal Controls and/or Instances of Noncompliance:***

### FINDING 02-FAC-21: The Finance And Administration Cabinet Should Ensure That Security Information Leakage For Agency Devices Is Minimized

FAC should restrict critical information divulged by their network servers. During our testing of the FAC local area network (LAN) security for FY 02, we discovered several instances where machines within the LAN provided information to anonymous users that could potentially divulge information that would assist in an unauthorized system attack.

Using standard scanning tools, we examined all machine names and other remarks for all machines located within the FAC domain. The naming convention of servers was not sufficiently ambiguous to disguise the function of several servers. Further, remarks available from two machines might catch an intruder's interest.

We also ran other vulnerability assessment tools twice during FY 02 on 37 servers within the FAC domain to determine if they would return information on Local Security Authority (LSA), Password Policies, Valid User, Group, or Share Lists. The first assessment revealed more than half of the servers would return information. However, as of the end of the fiscal year, this situation had improved significantly, as shown below in the table.

| Type of Information | Number of machines that remain vulnerable | Percentage of 37 machines |
|---|---|---|
| LSA | 27 | 73.0% |
| Password Policies | 5 | 13.5% |
| Valid User List | 5 | 13.5% |
| Valid Group List | 5 | 13.5% |
| Valid Share List | 5 | 13.5% |

We found four servers under FAC control that had port 2301 open. We were able to log onto the Compaq Insight Manager application on two (2) of these servers with the default administrator user ID and password. This access provides too much information to a potentially unauthorized individual.

For security purposes, detailed information concerning the specific servers or user accounts that contributed to these findings is being intentionally omitted from this comment. However, these issues were thoroughly documented and communicated to the appropriate agency personnel.

## FINANCIAL STATEMENT FINDINGS

***Other Matters Relating to Internal Controls and/or Instances of Noncompliance:***

### FINDING 02-FAC-21: The Finance And Administration Cabinet Should Ensure That Security Information Leakage For Agency Devices Is Minimized (Continued)

An agency's domain information accessible world wide through inquiry tools or default logons should be kept at a minimum. Agencies should ensure that information such as server location, accounts associated with the server, data residing on the server, and the server's role is not accessible to the public. To accomplish this, an agency can configure devices to not respond to certain types of inquiries, can use naming conventions that obscure the purpose of servers, can provide no comments on server activity, and can restrict access to default logons for applications.

**Recommendation**

We recommend that FAC restrict the information provided by its LAN machines to anonymous users. First, the naming convention for servers should be altered to make them more ambiguous and any unnecessary comments associated with the servers should be removed. Second, limitations should be placed on the type of response servers provide to system inquiries. Third, the default logons for the CIM application should be changed.

**Management's Response and Corrective Action Plan**

- *Machines comments on the two machines in questions have had the comments removed.*
- *As machines are being reloaded or replaced, they will be issued a new name from the standard naming convention of FINANXx. Current named machine are not scheduled for being renamed.*
- *FINANCE Office of Technology Services has taken steps to Protect LSA information and restrict Anonymous access, to the extent that the network can continue to function properly in communicating over the WAN with necessary GOT Services.*
- *Compaq Insight Manager Software was installed as a demonstration. It has been uninstalled. Other instances of Compaq Insight Services have been disabled if they were not needed. In the future FINANCE may enable this software to aid in monitoring the network and ensuring maximum availability of the FINANCE network servers and devices.*

## FINANCIAL STATEMENT FINDINGS

***Other Matters Relating to Internal Controls and/or Instances of Noncompliance:***

### FINDING 02-FAC-22: The Finance And Administration Cabinet Should Change System Defaults To Guard Against Unauthorized System Access

While performing interim system vulnerability tests at FAC, we found four (4) servers, or 10.8 percent of the 37 servers examined, that had the Simple Network Management Protocol (SNMP) service available and would allow an anonymous user to logon with the community name "public." The "public" community name is the default public account for this service. The use of the "public" community name allows too much information to be provided to any anonymous user. Through our testing the system provided information about listening ports, open sessions, active user accounts, and shares that exist. As of the end of the fiscal year, this vulnerability only existed for one server.

For security purposes, detailed information concerning the specific servers or user accounts that contributed to these findings is being intentionally omitted from this comment. However, these issues were thoroughly documented and communicated to the appropriate agency personnel.

Information provided by the SNMP service concerning a machine's functions could be useful to an intruder in developing an attack. Worldwide access through default logons should not be allowed. To accomplish this, the agency should change the SNMP service default community names.

#### Recommendation

We recommend FAC either disconnect the SNMP service or change the "public" community name to a more sophisticated name on all servers. Further, any new machines should be checked for the SNMP service to ensure the "public" community name has been changed.

#### Management's Response and Corrective Action Plan

*The Finance Cabinet will be using SNMP to monitor Server availability. The Community name will be verified on all machines and turned off of any that is not necessary for server monitoring.*

## FINANCIAL STATEMENT FINDINGS

***Other Matters Relating to Internal Controls and/or Instances of Noncompliance:***

### FINDING 02-FAC-23: The Finance And Administration Cabinet Should Strengthen Its Account Password Policy And Implement The Policy On All Domain Servers

During April 2002, FAC finalized and distributed policy statements for multiple security issues including criteria to be used to manage system accounts and passwords. This Account Password Policy (Policy) did not explicitly state the time period an account should be locked out after a number of unsuccessful logon attempts. Also, the Policy did not address account lockout reset standards for the agency. To review the compliance of FAC servers to this Policy, the auditor used industry standards for these two items.

Account related information was obtained from 24 servers within the FAC domain. This information was compared to Policy criteria or the industry standard. The results of this comparison are illustrated in the table below.

| Security Measure | Standard | Number of machines not in compliance with policy | Percentage of 24 machines not in compliance with policy |
|---|---|---|---|
| Maximum Password Age | 31 days | 20 – 42 days<br>2 – 999 days<br>1 – None | 95.8% |
| Minimum Password Age | 1 day | 24 – None | 100.0% |
| Minimum Password Length | 5 characters | 20 – None | 83.3% |
| Account Lockout Threshold | 5 attempts | 19 – None | 79.2% |
| Account Lockout Duration | "Forever" – Industry Standard | 21 – 30 minutes<br>2 – None | 95.8% |
| Account Lockout Reset | 1,440 minutes – Industry Standard | 21 – 30 minutes<br>1 – 720 minutes<br>2 – None | 100.0% |

The NetBIOS information from the primary domain controller was examined to determine if accounts adhered to the Policy. We found 14 user accounts that logged onto the system that did not comply with the FAC Policy to change an account password at least every 31 days. Further, the auditor examined NetBIOS information from six (6) other servers. Administrator accounts did not comply with the Policy on five (5) servers and Guest or User accounts on three (3) servers failed to meet the Policy requirements.

## FINANCIAL STATEMENT FINDINGS

***Other Matters Relating to Internal Controls and/or Instances of Noncompliance:***

**FINDING 02-FAC-23: The Finance And Administration Cabinet Should Strengthen Its Account Password Policy And Implement The Policy On All Domain Servers (Continued)**

For security purposes, detailed information concerning the specific servers or user accounts that contributed to these findings is being intentionally omitted from this comment. However, these issues were thoroughly documented and communicated to the appropriate agency personnel.

Passwords are a significant feature to guard against unauthorized system access. The failure to follow adequate Policy standards when establishing a system password could ultimately compromise the entire network. The purpose of a password policy is to establish a standard to create strong passwords, to protect those passwords, and to ensure passwords are changed within a specified time period. To assist in the security of a network, it is necessary for a strong Policy to be developed and consistently implemented on all servers throughout the network.

### Recommendation

We recommend FAC update their Policy to include standards for account lockout duration and account lockout reset. Further, the updated password policy should be implemented consistently on all FAC servers.

### Management's Response and Corrective Action Plan

*Finance Cabinet Current domain account policy is:*

| ***Security Measure*** | ***Standard*** | ***FINANCE*** |
|---|---|---|
| *Maximum Age* | *31 days* | *30 days* |
| *Minimum Age* | *1 day* | *Immediate* |
| *Minimum Length* | *5 characters* | *6 characters* |
| *Lockout Threshold* | *5 attempts* | *5* |
| *Lockout Duration* | *Forever* | *Forever* |
| *Lockout Reset* | *1,440 Minutes* | *1,440 Minutes* |

*FINANCE Office of Technology Services has taken steps to Protect LSA information and restrict Anonymous access, to the extent that the network can continue to function properly in communicating over the WAN with necessary GOT Services.*

## FEDERAL AWARD FINDINGS AND QUESTIONED COSTS

***Other Matters Relating to Internal Controls and/or Instances of Noncompliance:***

**FINDING 02-FAC-24: The Finance and Administration Cabinet Should Ensure The Agreement Between The United States Department Of The Treasury And The Commonwealth Is In Compliance With 31 CFR Part 205 – Cash Management Improvement Act**

Our audit of compliance with the Cash Management Improvement Act (CMIA) of 1990 for FY 02 reportable projects revealed three instances where the agreement between the United States Department of the Treasury and the Commonwealth (TSA) was not in compliance with 31 CFR Part 205 (CMIA). First, the flow of federal funds was not reviewed and updated within the TSA for FY 02. This information is used to determine the correct clearance pattern for CMIA eligible programs. A clearance pattern is prescribed for each CMIA eligible program to schedule the transfer of federal funds to the Commonwealth and to support the calculation of interest. If a designated clearance pattern does not reflect the actual flow of federal funds, the potential exists that interest due to or due from the federal government will unnecessarily accrue. Given section 7.4 of the TSA was not updated accordingly to reflect the flow of federal funds, no evidence exists that the clearance patterns prescribed to CMIA reportable projects are being maintained to accurately reflect the clearance patterns in use.

Second, the TSA did not provide the process used to develop or maintain clearance patterns. The Commonwealth should include a clear statement of the any assumptions, standards, or conventions used when converting data into the clearance pattern used to develop and maintain clearance patterns.

Third, Exhibit II, containing the dollar-weighted days of clearance for applicable agencies, contained inaccurate information. Each year an authorized individual should certify the accuracy of the information contained within this exhibit and provide the certification to FMS. During the end of FY 02, a program that calculates the dollar-weighted days of clearance was placed in production to generate current values. The TSA for FY 02 was certified prior to the creation of this program and, therefore, the information does not necessarily accurately reflect the information within the MARS system.

It should be noted that the federal government approved the TSA as written for the FY 02. They agreed to the clearance patterns and dollar-weighted days of clearance for applicable agencies. The CMIA Annual Report was based upon these guidelines and, it appears, the deficiencies noted above would not have had a material impact on the Annual Report for FY 02.

Ultimately, the accuracy and completeness of the information within the TSA is the responsibility of FAC. To ensure that the information to be reported annually to the United States Treasury under the requirements of the CMIA is correct and complete, FAC must practice diligence when preparing the TSA to ensure that the TSA is in compliance with the CMIA regulations.

## FEDERAL AWARD FINDINGS AND QUESTIONED COSTS

***Other Matters Relating to Internal Controls and/or Instances of Noncompliance:***

**FINDING 02-FAC-24: The Finance and Administration Cabinet Should Ensure The Agreement Between The United States Department Of The Treasury And The Commonwealth Is In Compliance With 31 CFR Part 205 – Cash Management Improvement Act (Continued)**

### Recommendation

We recommend that FAC implement the following:

- Determine the federal expenditures flow to ensure that the prescribed Clearance Pattern for CMIA eligible programs accurately reflect the flow of federal funds.
- Expand section 7.0 of the TSA to clearly indicate clearance pattern development process and any assumptions, standards, or conventions used in converting the federal flow of funds when developing or maintaining clearance patterns.
- Update Exhibit II of the TSA to accurately reflect the Dollar – Weighted Day of Clearance.

### Management's Response and Corrective Action Plan

- *For the 2003 Treasury State Agreement (TSA), the Division of Statewide Accounting Services (DSAS) has reviewed and updated the federal expenditure flow for CMIA eligible projects to ensure project clearance patterns are an accurate reflection of their federal expenditure flow.*
- *For the 2003 TSA, DSAS has updated section 7.0 of the TSA to describe the process for clearance pattern development. DSAS has included standards, methods, and calculations used in determining the appropriate clearance pattern designations and a reference for the procedures to update the clearance patterns to correspond to a program's clearance activity.*
- *For the 2003 TSA, DSAS has updated the dollar-weighted days of clearance section of Exhibit II.*

## FEDERAL AWARD FINDINGS AND QUESTIONED COSTS

***Other Matters Relating to Internal Controls and/or Instances of Noncompliance:***

### FINDING 02-FAC-25: The Finance And Administration Cabinet Should Review All Eligible Cash Management Improvement Act (CMIA) Transactions Requiring Interest Calculations To Ensure That The Annual Report Is Complete And Accurate

After reviewing the CMIA Annual Report for FY 02, it was concluded that the report is not complete or accurate as a result of a miscalculation of Direct Costs and the lack of a prior year interest adjustment by the Commonwealth.

During the review of the Direct Costs, we determined that the insurance rate per hour was miscalculated for FY 02. This error effects the calculation of interest activities as reported on the Direct Costs worksheets, which resulted in a variance of $95. As a result, the Interest Calculation Costs Report, which is part of the CMIA Annual Report, should reflect a total State Personnel Cost of $6,268 instead of $6,173.

In addition, a verbal comment was issued during FY 01 after an examination of the Federal Interest Liability determined that three (3) projects associated with CMIA Catalog of Federal Domestic Assistance (CFDA) #20.205 were incorrectly established in the MARS. It appears that these projects should have been associated with CFDA #20.219, which is not CMIA reportable. The documentation provided by FAC indicates 12 transactions existed in which federal interest was accrued for these projects. Therefore, the $996 that was paid to the Commonwealth for FY 01 should have been refunded to the federal government during FY 02; however, no prior year adjustment was made to the FY 02 Annual Report.

Ultimately, the accuracy of the CMIA Annual Report is the responsibility of FAC. To ensure that the Annual Report is correct, those responsible for the development of the Annual Report should review any transactions requiring the calculation of interest to ensure they are accurate. Further, a review of prior year adjustment should be made to ensure that all adjustments are included in the Annual Report.

#### Recommendation

We are recommending that FAC make the following corrections on the FY 03 Annual Report:

- An adjustment to Direct Cost Claims in the amount of $95
- A prior year adjustment of Federal Interest Liability for CFDA #20.205 of $996

#### Management's Response and Corrective Action Plan

*The Division of Statewide Accounting Services will make the adjustments as prescribed on the 2003 CMIA Annual Report.*

# SUMMARY SCHEDULE OF PRIOR AUDIT FINDINGS
## FOR THE YEAR ENDED JUNE 30, 2002

| Fiscal Year | Finding Number | Finding | CFDA Number | Questioned Costs | Comments |
|---|---|---|---|---|---|
| **Reportable Conditions** | | | | | |
| ***(1) Audit findings that have been fully corrected:*** | | | | | |
| FY 01 | 01-FAC-1 | The Office Of Financial Management Should Improve Daily Monitoring Of The Sweep Amounts | N/A | $0 | Resolved during FY 02. |
| FY 01 | 01-FAC-4 | The Office Of Financial Management Should Improve Security of Its Servers | N/A | 0 | Resolved during FY 02. |
| FY 01 | 01-FAC-5 | Catalog Of Federal Domestic Assistance Numbers Were Improperly Coded In MARS | N/A | 0 | Due to improvements, this finding is downgraded to an other matter for FY 02. This finding is no longer required to be reported under *Government Auditing Standards*. |
| ***(2) Audit findings not corrected or partially corrected:*** | | | | | |
| FY 01 | 01-FAC-2 | The Finance And Administration Cabinet Should Improve Controls Over Preparation Of The Cash And Investment Note | N/A | 0 | The cash and investment note preparation process has improved, but improvements are still needed in the classification and categorization areas.<br><br>See 02-FAC-2 |
| FY 01 | 01-FAC-3 | The Office Of Financial Management Should Improve Control Procedures Over Modifications To System Programs | N/A | $0 | Major processing programs were rewritten in audit period by new programmer on staff. However, the issue still remains.<br><br>See 02-FAC-3 |
| FY 01 | 01-FAC-6 | The Office of Technical Services Should Improve Security Of The Servers Within The Local Area Networks For Finance and Administration Cabinet. | N/A | 0 | Enterprise security improved but agency level security still noted as weak. Additional issues were identified in six (6) new findings during testing of FAC servers for FY 02. Three (3) of these findings are reportable conditions.<br><br>See 02-FAC-7, 02-FAC-8, and 02-FAC-9. |

# SUMMARY SCHEDULE OF PRIOR AUDIT FINDINGS
## FOR THE YEAR ENDED JUNE 30, 2002

| Fiscal Year | Finding Number | Finding | CFDA Number | Questioned Costs | Comments |
|---|---|---|---|---|---|
| **Reportable Conditions (Continued)** | | | | | |
| ***(2) Audit findings not corrected or partially corrected:*** | | | | | |
| FY 01 | 01-FAC-7 | The Finance And Administration Cabinet Should Implement Policies And Procedures To Ensure Compliance With Applicable Small Or Small Minority Business Set-Aside Laws | N/A | 0 | The Disparity Study was received by FAC in March 2003.<br><br>See 02-FAC-1 |
| FY 00 | 00-FAC-6 | The Office Of Financial Management Should Improve Control Procedures Over Modifications To System Programs | N/A | 0 | See 02-FAC-3 |
| FY 99 | 99-FAC-10 | The Finance And Administration Cabinet Should Implement Policies And Procedures Relating To Small Or Small Minority Business Set-Aside Laws | N/A | 0 | See 02-FAC-1 |

***(3) Corrective action taken is significantly different from corrective action previously reported:***

There were no findings to report for this section.

***(4) Audit finding is no longer valid or does not warrant further action:***

**Material Weaknesses**

***1) Audit findings that have been fully corrected:***

There were no findings to report in this section.

***(2) Audit findings not corrected or partially corrected:***

There were no findings to report in this section.

***(3) Corrective action taken is significantly different from corrective action previously reported:***

There were no findings to report in this section.

***(4) Audit finding is no longer valid or does not warrant further action:***

There were no findings to report in this section.

# SUMMARY SCHEDULE OF PRIOR AUDIT FINDINGS
## FOR THE YEAR ENDED JUNE 30, 2002

| Fiscal Year | Finding Number | Finding | CFDA Number | Questioned Costs | Comments |
|---|---|---|---|---|---|
| **Other Matters** | | | | | |
| ***(1) Audit findings that have been fully corrected:*** | | | | | |
| FY 01 | 01-FAC-9 | The Office Of Financial Management Should Review Procedures To Ensure Adequate Transaction Documentation Is Maintained | N/A | $0 | Resolved during FY 02. |
| FY 01 | 01-FAC-18 | The Finance and Administration Cabinet Should Ensure The Completeness and Accuracy of The Schedule of Interest Due From The Federal Government | N/A | 0 | Corrections were made as requested and no additional findings were noted for FY 02. |
| FY 01 | 01-FAC-19 | The Finance and Administration Cabinet Should Develop A Policy Concerning The Usage And Restrictions Surrounding The Government Wide Project Number Feature | N/A | 0 | Policies were provided that state an agency is not required to use the same CFDA number under a single GWPN. |
| ***(2) Audit findings not corrected or partially corrected:*** | | | | | |
| FY 00 | 00-FAC-7 | The Finance And Administration Cabinet Should Work In Conjunction With The Governor's Office For Technology To Implement Logging And Audit Features Within Procurement Desktop | N/A | 0 | Resolution still in progress.<br><br>See 02-FAC-17 |
| FY 01 | 01-FAC-8 | The Office Of Financial Management Should Improve MARS Reconciliation Procedures | N/A | 0 | MARS and CAMRA were not reconciled for three (3) months.<br><br>See 02-FAC-11 |
| FY 01 | 01-FAC-10 | The Finance and Administration Cabinet Should Ensure Agencies Follow The Closing Package Instructions Relating to Contingencies | N/A | 0 | See 02-FAC-14 |
| FY 01 | 01-FAC-11 | The Finance and Administration Cabinet should develop and Implement formal written policies and procedures concerning security of the Financial Analysis System | N/A | 0 | Still pending resolution. (scheduled to be incorporated in design changes for FAS.V2)<br><br>See 02-FAC-20 |

# SUMMARY SCHEDULE OF PRIOR AUDIT FINDINGS
## FOR THE YEAR ENDED JUNE 30, 2002

| Fiscal Year | Finding Number | Finding | CFDA Number | Questioned Costs | Comments |
|---|---|---|---|---|---|
| **Other Matters (Continued)** | | | | | |
| ***(2) Audit findings not corrected or partially corrected: (Continued)*** | | | | | |
| FY 01 | 01-FAC-12 | The Finance and Administration Cabinet should improve logical security measures over the Financial Analysis System | N/A | $0 | Still pending resolution (scheduled to be incorporated in design changes for FAS.V2)<br><br>See 02-FAC-19 |
| FY 01 | 01-FAC-13 | The Finance and Administration Cabinet should consistently apply established program modification control procedures for the Financial Analysis System | N/A | 0 | Still pending resolution (scheduled to be incorporated in design changes for FAS.V2)<br><br>See 02-FAC-18 |
| FY 01 | 01-FAC-14 | The Finance and Administration Cabinet should develop formal procedures for system assurance efforts concerning the Financial Analysis System | N/A | 0 | Still pending resolution (scheduled to be incorporated in design changes for FAS.V2)<br><br>See 02-FAC-16 |
| FY 01 | 01-FAC-15 | The Finance And Administration Cabinet Should Work In Conjunction With The GOT To Implement Logging And Audit Features Within Procurement Desktop | N/A | 0 | Resolution still in progress.<br><br>See 02-FAC-17 |
| FY 01 | 01-FAC-16 | The Finance and Administration Cabinet Should Ensure The Treasury – State Agreement Is In Compliance With 31 CFR Part 205 – Cash Management Improvement Act | N/A | 0 | There were issues again noted with the TSA for FY 02. New issues were added for FY 02 due to the need to comply with the revised CFR.<br><br>See 02-FAC-25 |
| FY 01 | 01-FAC-17 | The Finance and Administration Cabinet Should Monitor Cash Management Improvement Act Eligible Projects To Ensure They Are Properly Recorded In MARS | N/A | 0 | Significant improvements were made to the number of exceptions noted for FY 02. This comment has been downgraded to a verbal for FY 02. |

***(3) Corrective action taken is significantly different from corrective action previously reported:***

There were no findings to report in this category.

***(4) Audit finding is no longer valid or does not warrant further action:***

There were no findings to report in this category.